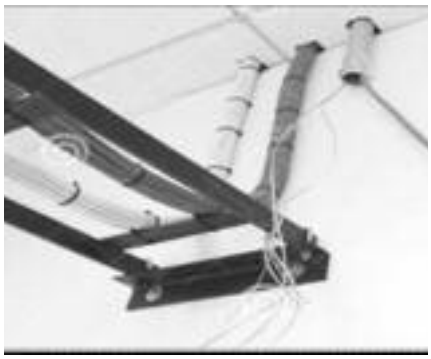
ওয়াই-ফাইয়ের নিরাপত্তা বাড়ানোর উপায়

সম্প্রতি ওয়্যারলেস নেটওয়ার্কের ব্যবহার ব্যাপকভাবে বেড়ে গেছে। আর তাই হোম বা অফিস যেকোনো পর্যায়ে ওয়্যারলেস নেটওয়ার্কের সর্বোচ্চ নিরাপত্তা নিশ্চিত করা প্রয়োজেন। এ লেখায় ওয়্যারলেস নেটওয়ার্কে আড়ি পাতা ও ভাইরাস আক্রমণ প্রতিরোধ করাসহ আরও বেশ কিছু নিরাপত্তা সম্পর্কিত বিষয়ে আলোচনা করেছেন **কে এম আলী রেজা**।

আমরা অনেক সময় মনে করি, ওয়্যারলেস ল্যানের বা নেটওয়ার্কের এনক্রিপশন (encryption) ফিচার চালু করলেই নেটওয়ার্কের নিরাপত্তা নিশ্চিত হয়ে যায়। কিন্তু উন্নত প্রযুক্তি জ্ঞানসম্পন্ন ওয়াই-ফাই হ্যাকারেরা এ ধরনের ব্যবস্থা ভেঙ্গে ওয়্যারলেস নেটওয়ার্কে অনুপ্রবেশ করতে পারে এবং নেটওয়ার্ক ব্যবস্থায় বিভিন্ন ধরনের অনিষ্ট সাধন করতে পারে।

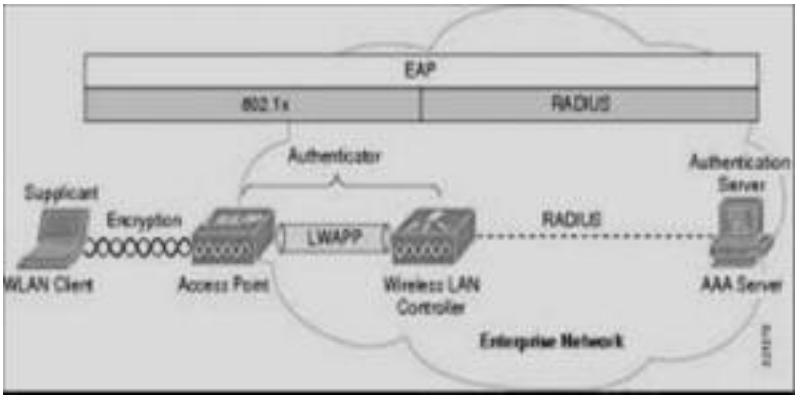
নেটওয়ার্কের ফিজিক্যাল নিরাপত্তা

ওয়্যারলেস নেটওয়ার্কের ফিজিক্যাল নিরাপত্তা একটি গুরুত্বপূর্ণ বিষয়, যদিও আমরা এ বিষয়টিকে অনেক সময় যথাযথ গুরুত্বের সাথে বিবেচনা করি না। আমাদের অসাবধানতার কারণে জ্ঞাতসারে বা অজ্ঞাতসারে নেটওয়ার্কের অনুমোদিত ইউজার বা বাইরের ইউজারের মাধ্যমে ওয়াই-ফাই ডিভাইস এবং নেটওয়ার্ক হার্ডওয়্যারের অপব্যবহার হতে পারে। উদাহরণস্বরূপ, আমরা যদি নেটওয়ার্ক জ্যাক অসাবধানবশত খোলা রাখি, তাহলে যেকোনো ইউজার তার নিজস্ব এক্সেস পয়েন্ট (এপি)-এর সাথে জ্যাকটি সংযুক্ত করে তার নিজস্ব ওয়াই-ফাই নেটওয়ার্কের শক্তি বাড়াতে পারে। এ ইউজার হয়তো এক্সেস পয়েন্টকে বহিরাগতদের অনুপ্রবেশ নিবৃত্ত করতে তথা নেটওয়ার্ক সিকিউরিটি প্রদানে যথাযথ ব্যবস্থা নেবে না। এছাড়া কেউ হয়তো উদ্দেশ্যপ্রণোদিতভাবে এক্সেস পয়েন্ট বা রাউটারকে ফ্যাক্টরি ডিফল্ট সেটিংয়ে রিসেট করে দিতে পারে। এর ফলে ওয়াই-ফাইয়ে'র সিকিউরিটি সেটিংগুলো অকার্যকর হয়ে যাবে। এ অবস্থায় ওয়াই-ফাই সীমার মধ্যে অননুমোদিত ইউজারেরা নেটওয়ার্কে এক্সেস পেয়ে যাবে।



কনডুইটের মাধ্যমে নেটওয়ার্ক ক্যাবল সুরক্ষা করা

ওয়্যারলেস নেটওয়ার্কের ফিজিক্যাল উপাদানগুলোর সুরক্ষার জন্য এগুলোকে এমন জায়গায় স্থাপন করা প্রয়োজন যাতে তা সাধারণ ইউজার ও বহিরাগতদের নজরে না আসে। নেটওয়ার্ক বিশেষ করে ইথারনেট ক্যাবল দেয়ালের ভেতর দিয়ে টানা প্রয়োজন। ক্ষেত্র বিশেষে ক্যাবলগুলো কোনো মোড়কের (কনডুইট) ভেতরে স্থাপন করা যেতে পারে। ইথারনেট জ্যাক নিরাপদ জায়গায় স্থাপন করতে পারেন যাতে এগুলোর এক্সেস যেন কেউ না পায়। নেটওয়ার্কের অপ্রয়োজনীয় জ্যাকগুলো নিষ্ক্রিয় করে দিতে হবে।



নেটওয়ার্ক সুরক্ষায় রেডিয়াস সার্ভারের ব্যবহার

৮০২.১এক্স (802.1X) অথেনটিকেশনসহ এন্টারপ্রাইজ সিকিউরিটি ব্যবহার

অনেকেই অবগত আছেন, ওয়্যারলেস নেটওয়ার্কের WEP (Wired Equivalent Privacy) সিকিউরিটি ব্যবস্থা সহজেই ভেঙ্গে ফেলা যায় এবং এর ভেতর দিয়ে অননুমোদিত ইউজারেরা নেটওয়ার্কে এক্সেস নিতে পারে। এ কারণে ওয়্যারলেস নেটওয়ার্কে WPA এবং WPA2 (Wi-Fi Protected Access) ব্যবস্থা ব্যবহার করা হয় পর্যাপ্ত সুরক্ষা পাওয়ার জন্য। তবে এ সুরক্ষা ব্যবস্থা ব্যবহারের দুটো ভিন্ন পদ্ধতি রয়েছে। এর মধ্য একটি হচ্ছে পার্সোনাল মোড (Personal mode) যার সেটআপ এবং ব্যবহার খুব সহজ। তবে কর্পোরেট বা বিজনেস নেটওয়ার্কের ক্ষেত্রে এ মোডটি ব্যবহার না করাটাই ভালো। বৃহৎ এবং স্পর্শকাতর নেটওয়ার্কের ক্ষেত্রে একটি গ্লোবাল স্ট্যাটিক পাসফ্রেজ (Passphrase) তৈরি করে তা এন্ড-ইউজার ডিভাইসে সংরক্ষণ করা হয়। এ পদ্ধতি এন্টারপ্রাইজ মোড হিসেবে পরিচিত। যদি কোনো ইউজার প্রতিষ্ঠান ছেড়ে যায় বা এন্ড-ইউজার ডিভাইস চুরি হয়ে যায়, তাহলে সেক্ষেত্রে সব এক্সেস পয়েন্ট এবং এন্ড-ইউজার ডিভাইসে গ্লোবাল পাসফ্রেজ পরিবর্তন করতে হয়।

তুলনামূলকভাবে এন্টারপ্রাইজ (Enterprise) মোড সেটআপ প্রক্রিয়া জটিল এবং এজন্য RADIUS (**Remote Authentication Dial-In User Service**) অথেনটিকেশন সার্ভার বা সার্ভিসের প্রয়োজন হয়। তবে এটি নেটওয়ার্কের সর্বোত্তম নিরাপত্তা নিশ্চিত করে। এ পদ্ধতিতে প্রত্যেক ইউজারের জন্য ইউনিক লগইন ক্রেডেনশিয়াল (ইউজার নেম ও পাসওয়ার্ড) নির্দিষ্ট করে দেয়া হয় এবং তা প্রয়োজনে সহজেই পরিবর্তন করা যায় বা প্রত্যাহার করে নেয়া হয়। কোন ইউজার কোম্পানী ত্যাগ করলে বা ওয়্যারলেস ডিভাইস হাতছাড়া হয়ে গেলে তার জন্য নির্ধারিত লগইন ক্রেডেনশিয়াল প্রত্যাহার করা হয়। এতে একজন ইউজার অন্য ইউজারের ডাটা ট্রাফিক সম্পর্কে কোন তথ্য জানতে পারে না, যা পার্সোনাল মোডে সম্ভব হয়।

৮০২.১এক্স (802.1X) ক্লায়েন্ট সেটিংয়ের নিরাপত্তা বিধান

WPA বা WPA 2 নিরাপত্তা সিস্টেমে এন্টারপ্রাইজ মোড অধিকতর মজবুত. তারপরও এতে কিছু নিরাপত্তা ঘাটতি রয়েছে। উদাহরণস্বরূপ ইউজারের লগইন নাম ও পাসওয়ার্ড বাইরের কেউ জেনে যেতে পারে। অনেক সময় এগুলো হ্যাকিংয়ের শিকার হতে পারে। তবে এন্ড-ইউজার ডিভাইসে ক্লায়েন্ট সেটিংয়ের মাধ্যমে লগইন ক্রেডেনশিয়াল ডাটাবেজে বাইরের আক্রমণ প্রতিহত করা যায়। ক্লায়েন্ট পিসিতে এবং একে সাপোর্ট করে এমন সব ডিভাইসে ▸

নিশ্চিত করতে হবে যেন সার্ভার ভেলিডেশন ফিচারটি সক্রিয় থাকে।

নেটওয়ার্ক ঝুঁকি ও স্পর্শকাতরতা সম্পর্কে ইউজারদেরকে সচেতন করা

নেটওয়ার্ক সুরক্ষা রাখতে নেটওয়ার্ক অ্যাডমিনিস্ট্রেটর হিসেবে আপনার অনেক দায়িত্ব থাকে, একই সাথে ইউজারেরাও সুরক্ষায় অনেক গুরুত্বপূর্ণ অবদান রাখতে পারে। ইউজারদেরকে সুরক্ষার বিষয়ে প্রশিক্ষিত করা এবং নেটওয়ার্ক ব্যবহারের বিষয়ে একটি কার্যকর নীতিমালা প্রণয়নের মাধ্যমে আপনি একটি ওয়্যারলেস নেটওয়ার্ককে নিরাপদ রাখতে পারেন। নেটওয়ার্ক অ্যাডমিনিস্ট্রেটর ইউজারদের পরামর্শ দিতে পারে তারা যেন নেটওয়ার্কে কোন ডিভাইস সংযুক্ত বা বিচ্ছিন্ন করার আগে অ্যাডমিনিস্ট্রেটরের অনুমতি গ্রহণ করে। এছাড়া নেটওয়ার্কের নিরাপত্তার স্বার্থে আশপাশের ওয়াই-ফাই নেটওয়ার্কে যুক্ত না হওয়া, অফিসে কোনো ল্যাপটপ বা মোবাইল ডিভাইস হারিয়ে গেলে তা সাথে সাথে নেটওয়ার্ক অ্যাডমিনিস্ট্রেটরকে জানানো, নেটওয়ার্ক রিসোর্স শেয়ারিংয়ের বিষয়ে সতর্কতা অবলম্বন ইত্যাদি বিষয়ে ইউজারদেরকে সচেতন করা যেতে পারে।

ইউজার পিসিতে ওয়াই-ফাই সুবিধা সীমিত রাখা

নেটওয়ার্কভুক্ত যেসব পিসিতে উইন্ডোজ ভিসতা বা তার পরবর্তী ভার্সনের অপারেটিং সিস্টেম চালু রয়েছে সেগুলোতে পার্শ্ববর্তী অন্যান্য ওয়্যারলেস নেটওয়ার্ক নামগুলো *(SSID*-service set identifier*)* ব্লক বা বন্ধ করে দেয়া যেতে পারে। কমান্ড প্রম্পটে *netsh wlan* কমান্ড ব্যবহার করে ফিল্টার তালিকায় ওই পার্শ্ববর্তী নেটওয়ার্কের নাম যুক্ত করতে পারেন যাতে ইউজারেরা ওই নেটওয়ার্কে এক্সেস থেকে বিরত থাকে।

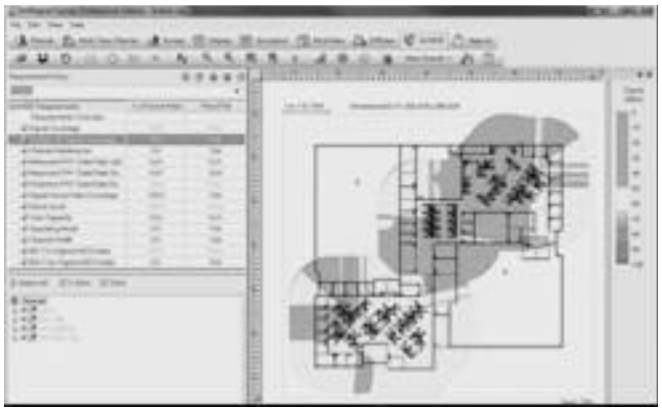
মাইক্রোসফট তার উইন্ডোজ ৭ এবং উইন্ডোজ সার্ভার ২০০৮ (রিলিজ ২) অপারেটিং সিস্টেমে Wireless Hosted Networks নামে একটি ওয়াই-ফাই ফিচার যুক্ত করেছে। এর সাহায্যে ইউজার একটি ভার্চুয়াল এক্সেস পয়েন্ট (এপি) তৈরি করতে পারে, যা অন্য ইউজারের কাছে উন্মুক্ত হতে পারে। তবে নেটওয়ার্কের নিরাপত্তার স্বার্থে ইউজারেরা যাতে এই ফিচারের সাহায্যে এক্সেস পয়েন্ট তৈরি করে নেটওয়ার্কে ঝুঁকির মধ্যে না ফেলতে পারে সেজন্য সার্ভারের গ্রুপ পলিসি রুলের আওতায় সুবিধাটি বন্ধ করে দেয়া যেতে পারে।

ওয়াই-ফাই সাইট সার্ভে সম্পন্ন করা

ওয়্যারলেস নেটওয়ার্কের কর্মক্ষমতা এবং নিরাপত্তা অবস্থা মূল্যায়নের জন্য একটি নির্দিষ্ট সময় পর পর ওয়াই-ফাই সাইট সার্ভে করা প্রয়োজন। ল্যাপটপ বা মোবাইল ডিভাইস সাথে নিয়ে নেটওয়ার্কভুক্ত এলাকা ঘুরে ওয়্যারলেস সিগন্যালের শক্তি জানতে পারেন। এছাড়া স্থানীয় ওয়্যারলেস ইন্টারফেসে এক্সেস পয়েন্টের বৃত্তান্ত পাওয়া যায়। এছাড়া উইন্ডোজে inSSIDer বা এন্ডরোয়েড ডিভাইসে Wifi Analyzer প্রোগ্রামের সাথে নেটওয়ার্কের প্রাথমিক সার্ভে সম্পন্ন করা সম্ভব। উপরন্তু, নেটওয়ার্কে যেসব ইউজার অননুমোদিত এক্সেস পয়েন্ট তৈরি করতে পারে বা সিকিউরিটি সেটিং পরিবর্তন করে নেটওয়ার্কের নিরাপত্তা বিঘ্নিত করতে পারে তাদের বিষয়ে সতর্ক দৃষ্টি রাখতে হবে।

ওয়্যারলেস ইনট্রুশন প্রিভেনশন সিস্টেম (WIPS) ইনস্টল করা

অননুমোদিত বা ক্ষতিকার এক্সেস পয়েন্ট, নেটওয়ার্কে বাইরে থেকে ডিনায়েল-অব-সার্ভিস (DoS) অ্যাটাক ইত্যাদি প্রতিরোধে নেটওয়ার্কে ওয়্যারলেস ইনট্রুশন প্রিভেনশন সিস্টেম (WIPS) স্থাপন করা যেতে পারে। এ ধরনের সিস্টেমের ডিজাইন এবং ডিটেকশন টেকনিক ক্ষেত্রবিশেষে ভিন্ন ভিন্ন হতে পারে। সিস্টেম ইনস্টল করার পর এটি ওয়াই-ফাই নেটওয়ার্কের নিরাপত্তা অবস্থা সার্বক্ষণিক পর্যবেক্ষণ করতে থাকে। বেশ কিছু প্রতিষ্ঠান ওয়্যারলেস ইনট্রুশন প্রিভেনশন সিস্টেম তৈরি এবং বাজারজাত করছে। এদের মধ্যে অন্যতম হচ্ছে AirMagnet এবং AirTight Neworks। এছাড়া ওপেন সোর্স যেমন Snort থেকেই এ সিস্টেম সংগ্রহ করা যায়।



চিত্র ৩: AirMagnet ওয়্যারলেস ইনট্রুশন প্রিভেনশন সিস্টেম

শেষ কথা

ওয়্যারলেস নেটওয়ার্ক সিস্টেম সুরক্ষার জন্য বেশ কয়েকটি পদ্ধতি এখানে আলোকপাত করা হয়েছে। তবে অ্যাডমিনিস্ট্রেটর হিসেবে সবার আগে নেটওয়ার্কের ফিজিক্যাল সিকিউরিটির বিষয়টি বিবেচনা করতে হবে। নেটওয়ার্ক সম্পর্কি ডিভাইস এবং ক্যাবলগুলো এমন জায়গায় রাখতে হবে যাতে সেগুলো সাধারণ ইউজার এবং বহিরাগতদের নজরে না আসে। বড় আকারের বিশেষ করে ব্যবসায়ী প্রতিষ্ঠানে এন্টারপ্রাইজ 802.1X নিরাপত্তা ব্যবস্থা স্থাপন করা প্রয়োজন। এছাড়া যেসব প্রতিষ্ঠান স্পর্শকাতর বা আর্থিক ডাটা নিয়ে কাজ করে তাদের সিস্টেমে 802.1X ক্লায়েন্ট সেটিং আবশ্যক। অননুমোদিত এক্সেস পয়েন্ট তৈরি করতে পারে বা সিস্টেম সেটিং পরিবর্তন করতে পারে এমন ইউজারদেরকে প্রতিহত করার জন্য নেটওয়ার্কের নিয়মিত সার্ভে প্রয়োজন। এছাড়া ক্ষেত্রবিশেষে নেটওয়ার্ককে আরো সুরক্ষিত করতে আপনি ওয়্যারলেস ইনট্রুশন প্রিভেনশন সিস্টেম ইনস্টল করতে পারেন কজ

ফিডব্যাক :
kazisham@yahoo.com